EXHIBIT B

Visto Mobile™

VMES Security White Paper

Visto Mobile™ Enterprise Server 5.2

Rel. 2

VISTO™ Your Freedom in Hand™

Exhibit B

Visto Mobile™ Enterprise Server Version 5.2 Security White Paper Rel. 2

Notice

This document, as well as all accompanying documents for this product, is published by Visto Corporation and/or its subsidiaries (collectively, “Visto”). Visto may have patents or pending patent applications, trademarks, copyrights, or other intellectual property rights covering the subject matter in these documents. The furnishing of this, or any other document, does not in any way imply any license to these or other intellectual properties, except as expressly provided in written license agreements with Visto Corporation. This document is for its intended recipients only. No part of this document may be used, sold, reproduced, stored in a database or retrieval system or transmitted in any form or by any means, electronic or physical, for any purpose, other than the recipient’s authorized use without the express written permission of Visto Corporation. Any unauthorized copying, distribution or disclosure of information is a violation of copyright laws.

While every effort has been made to ensure technical accuracy, information in this document is subject to change without notice and does not represent an obligation on the part of Visto Corporation to maintain the accuracy of this information. The software described in this document will only be furnished under a license agreement or nondisclosure agreement. The software may be used or copied only in accordance with the terms of those agreements.

Notice of Copyright, Trademarks and Patents

Third Party Marks

All third-party trademarks, trade names, or service marks used herein are the property of their respective owners and are used only to refer to the goods or services identified by those third-party marks.

P/N 52-0121-A4

© Visto Corporation
275 Shoreline Drive
Suite 300
Redwood City, CA, USA 94065
Tel: +1 (650) 486-6000
Fax: +1 (650) 622-9590
www.visto.com

Exhibit B

Table of Contents

Exhibit B

Table of Figures

List of Tables

Exhibit B

1. Overview

The Visto Mobile™ Enterprise Server (VMES) solution enables remote access to enterprise data sources and ISP e-mail accounts from a variety of wired and wireless terminal platforms. This white paper discusses the security architecture and security features of VMES. It addresses the key security concerns that enterprises may have regarding mobile access to enterprise data via VMES.

VMES provides the utmost security for important user and enterprise data. The best aspects of existing, commercially available methods for securing information that travels the Internet are utilized to ensure that extending mobile access to personal and enterprise data is not a security risk.

Given that confidentiality is one of the highest profile aspects of data security in a computing system, it is worth emphasizing here the following two points regarding the VMES solution. First, confidentiality and integrity is ensured through the use of Transport Layer Security (TLS) and Wireless Transport Layer Security (WTLS). In addition, enterprise data access via Visto's ConstantSync™ terminal clients is secured through the use of secure key exchange (using the ECDH algorithm) and end-to-end data encryption (using 128-bit AES). This use of end-to-end encryption closes the potential for confidentiality "WAP-gap" for enterprise data transmitted through the Visto Network Operations Center (NOC) to and from the ConstantSync clients.

However, data confidentiality is only one of many aspects of computing system security. In the balance of this whitepaper, system security is described through a discussion of the methods used by VMES to protect:

- User data
- Access to the enterprise network
- Access to the Visto Network Operations Center (NOC)

Securing access to data and the data itself is described by addressing how VMES handles:

- Authorization for and authentication of users to access VMES
- Storage of user profile data within the NOC
- Protection of information by encrypting data that travels the Internet
- Password management
- NOC physical, network, and application security

Exhibit B

2. Solution Architecture

The VMES solution is based on a real-time architecture for accessing enterprise data and ISP e-mail data from a broad array of mobile devices. VMES can be easily and rapidly deployed, minimizing infrastructure configuration and deployment costs. All components are designed from the ground up to provide enterprise-caliber security and carrier-grade reliability, availability, and scalability.

2.1 Architecture Overview

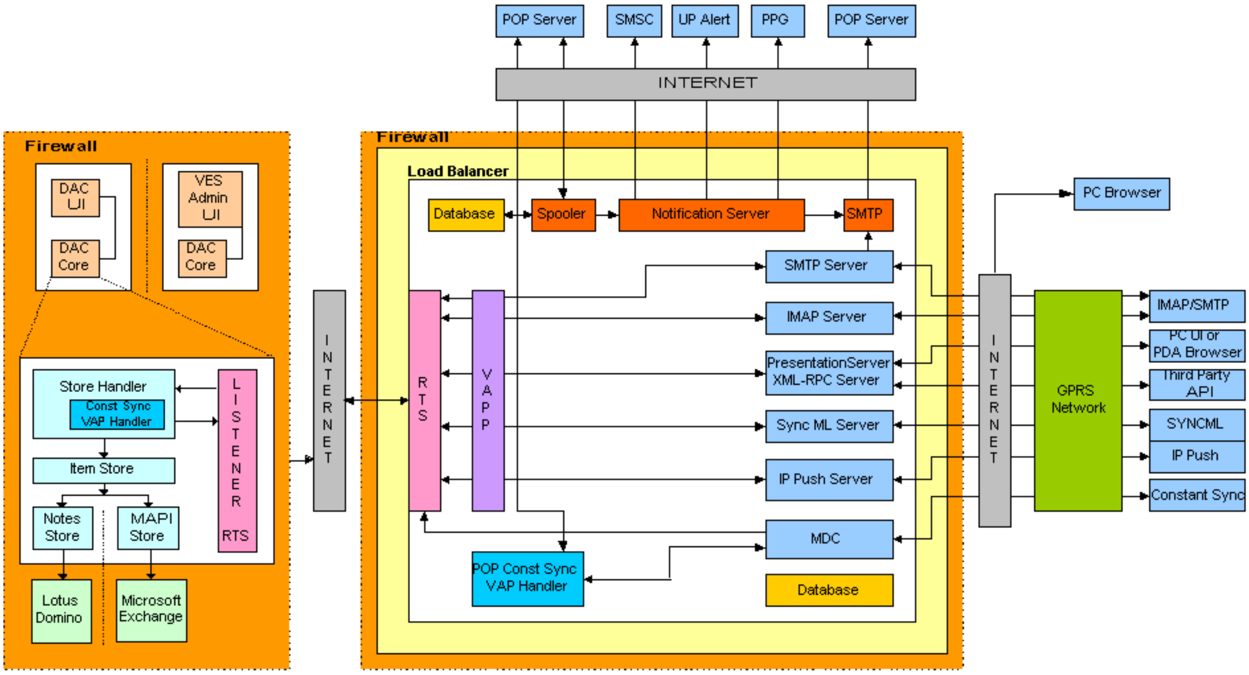

Figure 1: Visto Architecture

The Visto Mobile™ solution consists of three main components:

- Visto Enterprise Server: A behind-the-firewall component that integrates with an enterprise groupware server – Microsoft® Exchange or IBM® Lotus® Domino®
- Terminal Client on a wired PC or mobile wireless PC or device
- Visto Network Operations Center (NOC): A centrally hosted set of servers that manages secure real-time data access, data push parameters, ISP e-mail access, and billing/reporting activities

2.1.1 Visto Enterprise Server

The Visto Enterprise Server (VES) is a behind-the-enterprise firewall component that interfaces directly with an enterprise groupware server (Exchange or Domino) and with the Visto NOC. VES handles the credentials and connections necessary to access user data on the groupware server. (User enterprise network credentials or Exchange/Domino credentials are never stored at or transmitted through the NOC or anywhere else outside the enterprise firewall.) VES also maintains one or more connections to the NOC, over which it sends data to and receives data from terminals and devices controlled by the users it is configured to service.

2.1.2 Terminal Client

A VMES terminal client may be a PC-based web browser, a mobile-device-based browser, or a specialized terminal client that allows remote offline access to previously synchronized data.

The terminal client initiates SSL/TLS protected connections to the Visto NOC and sends a user's Visto service credentials (which consist of a MSISDN or e-mail address along with a password) to the NOC to identify and authenticate the user. Through the terminal client interface, a user may interact with data fetched from or sent to VES or an ISP e-mail server via the NOC.

The Visto ConstantSync clients represent a special subclass of supported terminal clients. All e-mail and PIM data exchanged between VES and a Visto ConstantSync terminal client is encrypted end-to-end using AES.

2.1.3 NOC

The Visto NOC authenticates connections from terminal clients and from VES installations and mediates communication between these endpoints. The NOC also initiates connections to ISP e-mail servers on behalf of users and mediates communication between terminal clients and these servers. No end-user application data (e-mail, appointments, contacts, etc.) is stored at the NOC.

For a detailed discussion of the operation and interaction of these VMES solution components and the various subcomponents shown in Figure 1 above, refer to the *Visto Mobile™ Technical Overview.*

Exhibit B

3. Visto Enterprise Server (VES)

A key component of the Visto Mobile Enterprise Server solution is the Visto Enterprise Server (VES), an enterprise-class server that manages the flow of information between a corporation's Microsoft Exchange or Lotus Domino server(s) and the Visto NOC or the device endpoint (Figure 2). It provides a central point of control for the corporation's IT management to manage user provisioning of the service. This is both a security benefit as well as a cost savings for large deployments in the enterprise, as there is no desktop software to manage.

3.1 Windows Service Component

VES is implemented to leverage the security infrastructure of the Windows operating system and that of the groupware servers with which it interacts. VES is installed on a Windows Server that resides on a company's local area network (LAN) and runs as a Win32 service. Configuration of this service requires that the IT administrator installing VES create a Windows account known as the VES administrative account. The VES administrative account is granted rights as a local administrator of the server on which VES runs and must be given certain administrative permissions on the groupware server(s) that VES will access.

The VES application does not directly store or manage the Windows credentials of the VES administrative account. The VES Win32 service is configured to "log on as" the VES administrative account. The credentials of that account are stored and maintained by the Windows service management system.

3.2 Administrative Interface

The VES administrative interface is implemented as a Microsoft Management Console (MMC) snap-in. The VES MMC interface must be run locally on server on which the VES service is installed and running.

Access to the VES administrative interface may be restricted simply by restricting access to local administrator credentials for the VES server. However, it is good practice also to restrict physical access to the VES server and to allow logons to the VES server only for accounts with local administrator permissions.

3.3 Groupware Server Access

E-Mail and PIM data is not stored on the VES or the Visto NOC. This data is stored only on the original messaging/groupware server and the synchronization-based (a.k.a., non-browser) terminal clients.

3.3.1 Microsoft Exchange Server

To enable the use of VES with Microsoft Exchange Server, a mailbox for the VES administrative account must be created on one of the Exchange servers that VES will access. The VES administrative account must also be granted full information store access on each of the Exchange servers with which it will interact. This setup procedure is described in detail in the *Visto Mobile™ Enterprise Server Installation and Administration Guide*.

Using the credentials of the VES administrative account, VES connects to Exchange servers using the Microsoft Messaging Application Programming Interface (MAPI) to access users' accounts. VES does not store or make use of Windows credentials for individual users.

3.3.2 IBM Lotus Domino Server

To enable the use of VES with Lotus Domino Server, a VES administrative account must be created on the Domino servers that VES will access. The VES administrative account must be granted administrative access to the templates and databases that VES will interact with. If VES and the Domino server reside in different domains, Domino must have a two-way trust relationship with VES. This setup procedure is described in detail in the *Visto Mobile™ Enterprise Server Installation and Administration Guide*.

Using the credentials (user id file and password) of the VES administrative account, VES accesses Lotus Domino servers using the Lotus Notes C API. VES does not store or make use of Lotus Domino credentials for individual users. The Domino password for the VES administrative account is stored encrypted in the Windows registry.

Following IBM recommendations, VES achieves scalable event detection for Domino by installing a Java agent for each provisioned user's mailbox to accept event notifications. These notifications are passed back to VES over a TCP/IP connection.

3.3.2.1 Domino VES Administrative account

The VES administrative account must be granted access to Domino e-mail databases and the Notes address book. However, Visto recommends that this account be given more restricted permissions than that of a full Domino administrator:

1. The VES administrative account requires access to only those users that will be provisioned on VMES (a full Domino administrator has access to all users).
2. The VES administrative account must have Editor rights to these users' mailboxes (a full Domino Administrator has Manager rights to user mailboxes).

Use of a separate VES administrative account with restricted access rights has the following advantages:

1. The Domino Administrator may separately track use of the VES administrative account.
2. The VES administrator requires physical access to the VES machine and Windows credentials for the VES administrative account. This in turn gives the VES administrator access to the Domino user id file and the associated password for the VES administrative account, but does not give access to the user id file and password for the Domino administrator.

The VMES is designed to use any user id with required administrative privileges (as described by the VMES installation document). Although a Domino administrator with maximum privileges can be used, a restricted access is recommended. The data access abilities by VMES administrator is less then the Domino Administrator access of the data.

The VMES administrator (as Domino administrator) will have access to the user information.

3.3.2.2 VES as a Notes Client Application

VES is a Notes client application (rather then a server application). Some differences between a Notes client and a Domino server application are as follows.

Notes Client application:

1. The client application requires a user id (the VES administrative account id) with restricted access compared to a Domino administrator ID or server ID.

2. The VES administrative account is used to provision users.

3. The client application relies on the notes client communication protocols and security to communicate with the Domino server.

Exhibit B

4. For notification, VMES uses the IBM recommended Java agent technology to notify the application for any changes in the users' documents. The agents are thin clients that process information on the Domino server in a secure environment.

Domino Server application:

1. The server based application requires a separate installation of the Domino server (any bug on the extension manager can potentially crash the Domino server). It also requires a purchase of a Domino server license.
2. Domino Administrator provisions the users. The users' data is accessed by the unrestricted server id. The users are provisioned using the Domino administrator.
3. The server application relies on the Domino server-to-server communication protocols and security.
4. Notifications are generated by the extension managers (a DLL is installed on the Domino server).
5. Any issues / bugs in the server application can cause issues on the domino server (expected risk / crash of domino server).

3.4 Licenses and Installation

VES installs in minutes on a Microsoft Windows server. Installation requires local administration privileges on the host server as well as the credentials for the VES administrative account described in Section 3.3. Before VES runs, the administrator is prompted for a license name and password issued to an enterprise at the time a VMES license is purchased. A VMES license may restrict the number of user accounts that can be provisioned for an enterprise. In general, multiple VES installations are allowed as long as the total user count for all associated installations does not exceed the amount allowed for the license.

After the license credentials are entered, VES connects using SSL to the NOC and submits the credentials for verification. If the credentials match those recorded in the NOC license table, a token representing the license is returned. This token (the license ID) is used by VES to authenticate itself as a VES belonging to the enterprise license when it later registers itself as a Real Time Service (RTS) client (see Section 4).

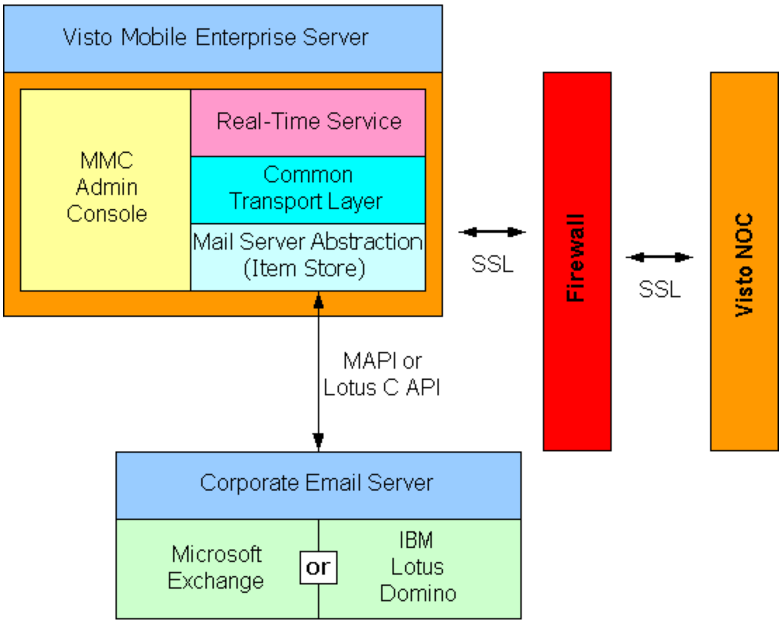

Figure 2: Visto Enterprise Server Block Diagram

Exhibit B

3.5 User Account Provisioning

The VES administrative interface is used to manage user accounts for the VMES service. User accounts can be added, modified, or deleted only by someone logged in to the VES server console as a user with the privileges of the VES administrative account.

Each user account is assigned a unique VMES username and a password. (The VMES solution does not require nor make use of the enterprise Windows or Domino credentials for individual users.) The username is the user's SMTP address. The password is a case-sensitive alphanumeric string that can either be randomly generated by VES upon provisioning or manually specified by the VES administrator, depending on the enterprise policy of each company. VES then sends these two account credentials (along with a first name and last name for the user) to the NOC via its RTS connection (see Section 4). The NOC stores the username and a hash of the account password to be used later for authentication of remote access by the user via browsers and other terminal clients. In addition, as each new user account is created, a check is made against the license information database in the Visto NOC to ensure that the enterprise license permits the action. If the maximum number of users allowed for provisioning is exceeded, the user cannot be provisioned until another user has been deleted or the enterprise has upgraded the number of seats allocated to its license.

As each user account is provisioned, VES automatically sends a welcome e-mail to the user's Exchange or Domino mailbox. This e-mail provides instructions to the user and information about the user's VMES account. It usually contains the newly assigned username and password credentials for the account. These credentials are sensitive information and are sent only via the enterprise e-mail system, not the public Internet. However, any VMES administrator who would prefer to transmit these credentials to users in some other fashion, may customize the welcome e-mail not to include the user's VMES account password (or even the username for that matter).

3.6 User Account Activation

Upon receipt of the welcome e-mail, VMES users are asked to activate their account. This is done by navigating a web-browser to the URL link provided in the welcome e-mail. The user must log in to the activation web page interface using the credentials provided in the e-mail. If successful, the user will be asked to provide a mobile telephone number (MSISDN) to be associated with the account. If the associated wireless carrier has not approved the MSISDN for use with VMES, account activation may not be allowed. After activation is completed, both the MSISDN and the user's SMTP address will be usable interchangeably as the username for the account. Users are also asked to supply a preferred time zone to be used for the display of date and time information.

Users should immediately follow the instructions to activate their VMES account and should use the web interface to update their account passwords at that time and periodically thereafter.

Figure 3 details the VMES user account activation flow.

Exhibit B

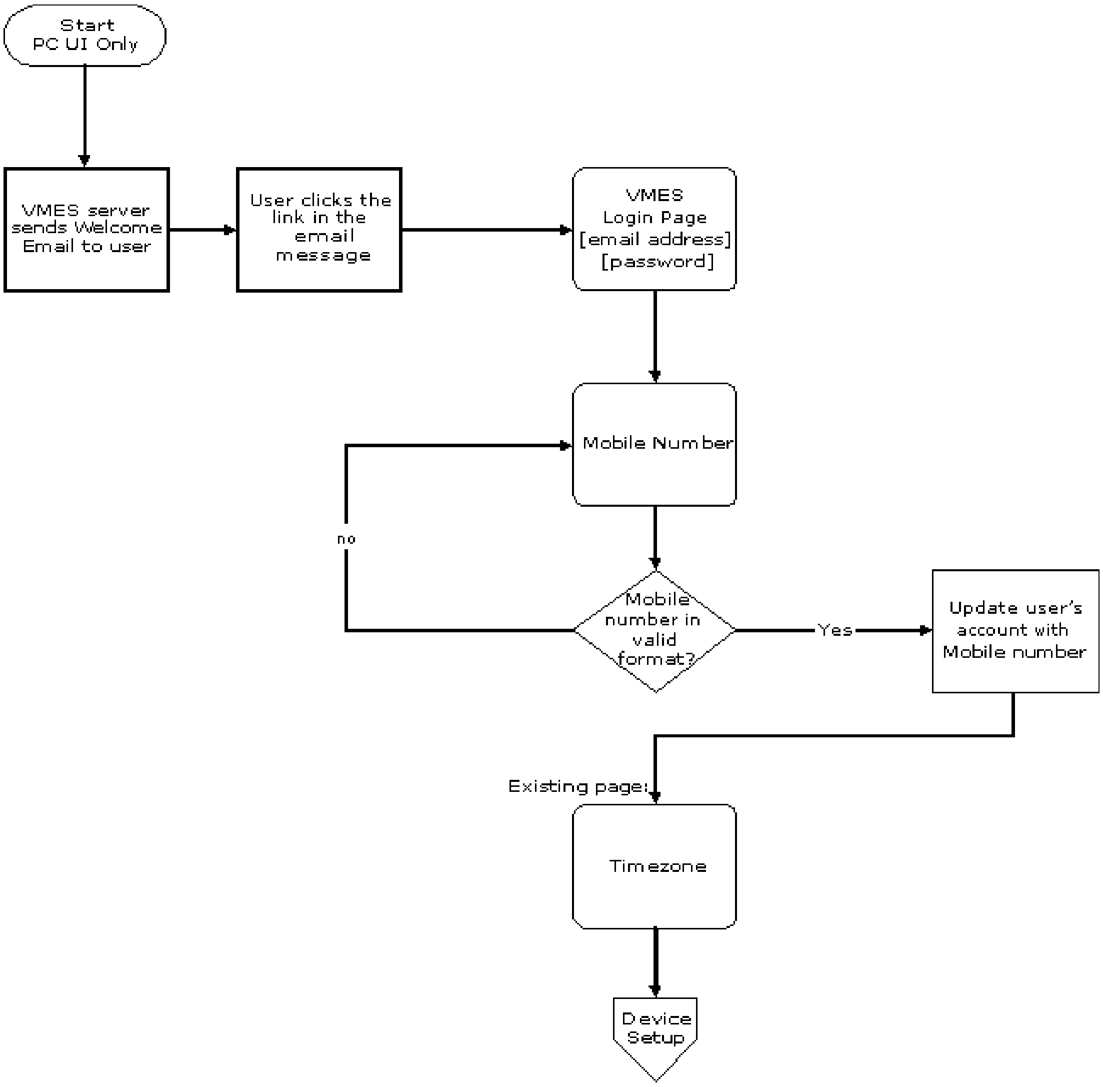
Start
PC UI Only
VMES server sends Welcome Email to user
User clicks the link in the email message
VMES Login Page [email address] [password]
Mobile Number
no
Mobile number in valid format?
Yes
Update user's account with Mobile number
Existing page:
Timezone
Device Setup

Figure 3: VMES Provisioning Flow

3.7 User Account Management

Once a user account is provisioned, the VES administrator, a Visto Customer Service Representative (CSR), or the user for whom the account was created may manage the account.

3.7.1 VES Administrator

From the MMC-based VES administration interface, the VES administrator may perform the following management tasks for provisioned user accounts.

1. Reset a user's password to a new value. VES will randomly generate a new password or the VES administration may set the password to some chosen string. (A new welcome e-mail is not sent to the user's Exchange or Domino account).

2. Delete the user from the VMES system.

The password-reset function is useful in the case that a user reports a forgotten password. It may also be used when a user reports a lost terminal client that has the old account password cached.

Resetting the account password will inhibit synchronization of any further user data to the lost terminal.

The delete user function is most useful to handle the case of a user that is no longer an employee of the enterprise. Deleting a user will inhibit synchronization of any further user data to terminals operated by the user and will prevent any further access by the user through any of the browser client interfaces.

The delete function may also be used to make room on a full license for new users by removing existing users that do not require data access via the VMES system.

3.7.2 Customer Service Representative

Visto Customer Service Representatives (CSRs) are not granted access to user e-mail and PIM data transmitted though the Visto NOC. CSRs are, however, granted the ability to manage user account settings in case the need should arise. The account management functions available to CSRs include the following functions:

- Grant activation approval to a particular MSISDN
- Search for existing user accounts
- Edit a user account profile
- Reset a user account password
- Reset a user account secret question
- Suspend or reactivate a user account
- Delete a user account
- Add or modify an ISP e-mail account configured for remote access through a VMES user account

The ability to edit a user account profile includes the ability to edit the stored first name, last name, MSISDN, and locale for an account. It also includes the ability to grant or block the ability of a user to access user data (e-mail, PIM, files, etc.) from any of the available interfaces (PC browse, PDA/WAP browse, IMAP/SyncML clients, ConstantSync clients). CRSs are *not* given access to the previously established values for user account passwords or to the passwords for any ISP e-mail accounts configured by the user.

The CSR interface and the security restrictions controlling access it are discussed in Section 8.

3.7.3 VMES user

From the PDA browse and WML browse interfaces, a VMES user may perform the following account management functions:

- Add or edit ISP e-mail account settings
- Select the e-mail account associated with synchronization-based terminal client access
- Turn e-mail alerts on or off
- Reset password (requires a secret question/answer to be previously set for the account)

From the PC browse interface, in addition to the above tasks, a VMES user may perform the following tasks:

- Edit the signature associated with each e-mail account for remotely composed e-mail
- Alter the number of days into the future for which calendar events are synchronized to terminal clients
- Create and edit e-mail alerts
- Edit quick text settings for remotely composed e-mail

Exhibit B

- Edit the first name, last name, contact e-mail address, and preferred time zone for the account
- Change the account password
- Set and edit a secret question and answer for the account

The Reset-password function can only be performed if the user has previously set a secret question and answer for the account, while logged in to the PC browse interface.

For a detailed walkthrough of the browse interfaces and further details on the features associated with the above account management functions, see the *Visto Mobile™ Browser and PC UI Reference Guide.* The security restrictions controlling access to the browse interfaces are discussed in Section 6.

3.8 Auditing and Monitoring

Auditing and monitoring of the VES server is possible due to its integration with the host Windows server. VES logs various administrative activities to the Windows event log. In addition, Windows auditing facilities may be configured to track administrative logons to the host server.

4. Real-Time Service Protocol

This white paper has so far covered the processes whereby a VES is installed, groupware servers are accessed, and user accounts are provisioned, activated and managed. The next step is to understand how VES provides secure access to enterprise data to users at remote sites.

4.1 Overview

The VES communicates with the Visto NOC through the enterprise firewall over the RTS protocol, utilizing HTTP over TLS (HTTPS). The "Real-Time Server" is so named because user data is transferred between VES and the terminal clients via the NOC in real time. The NOC does not employ a "store-and-forward" architecture. User data is retrieved only as needed and is not cached in the NOC database.

All communications with the NOC are over outbound HTTPS connections from the VES. VES does not communicate with the NOC via inbound connections, nor does it communicate with hosts outside the enterprise network other than those within the Visto NOC. The use of strictly outbound connections avoids the need for special enterprise firewall configuration by IT administrators. At installation, VES also automatically detects the presence of, and enables interoperation with, various enterprise proxies, including those requiring authentication. (For further details regarding VES connectivity requirements and deployment options, see Section 5.)

4.2 Design Motivations

There are a few major design motivations behind the RTS protocol:

- Provide a secure conduit for communications between VES and the Visto NOC
- Provide a protocol that can seamlessly pass through enterprise firewalls without requiring custom firewall configuration
- Limit data transfer between servers in the NOC

4.3 Command and Data Channels

An RTS session is established via an initial HTTPS connection, which the NOC responds to with a session key and a redirect URL. The RTS client (VES) then establishes a new HTTPS connection via the redirect URL, which is kept open and becomes the "command channel" – a downstream connection from the NOC.

The persistent command channel serves as the downstream connection from the NOC, but given the request-response nature of the HTTP protocol, it cannot be used as an upstream connection. When the client has data to send up to the NOC, it must establish a new HTTPS connection to post this data (sometimes referred to as the "data channel"). This temporary data channel connection persists only for the duration of the particular data request.

4.4 Authentication

A VES may not maintain multiple RTS sessions at a time. However, an RTS session often consists of more than one concurrent HTTPS connection. An RTS session includes one "Command Channel," which will be held open indefinitely (and re-established if dropped), and some number of temporary "Data Channel" connections (more than 20 simultaneous connections).

When the VES makes the initial connection for an RTS session to the NOC, the NOC response contains KeyID and Key parameters. The *KeyId* is the session identifier used to identify subsequent

Exhibit B

connections from the VES for the same RTS session. The *Key* parameter is a randomly generated 128-bit key used to authenticate subsequent connections from an RTS client for the same session.

VES generates a random 128-bit GUID for itself and registers itself with the NOC (during its initial RTS session) using the GUID and the license ID token. The VES GUID is treated as a shared secret between the NOC and the VES instance and is used to authenticate subsequent RTS sessions from the VES.

4.5 Connection Initialization

The RTS Connection procedure consists of multiple steps, as follows.

1. The RTS client (VES) makes a connection (HTTPS GET) to the Visto NOC via a URL that is built into the client.

2. The NOC produces a response containing several connection parameters, described as follows:

    - The *KeyId* parameter is session identifier used to identify subsequent connections from the VES for the same RTS session.
    - The *Key* parameter is a randomly generated 128-bit key used to authenticate subsequent connections from an RTS client for the same session.
    - The *EventUrl* parameter specifies the URL that the RTS client should use to establish the command channel connection.
    - The *ReplyTime* parameter specifies how long the NOC will wait for the client to reconnect before invalidating the session parameters.

3. The client reconnects to the NOC (HTTPS POST) using the *EventUrl KeyId,* and *Key* parameters specified in the NOC's response described above. The POST data of this HTTPS request contains an *RtsConnection* envelope, which specifies the GUID and the LicenseID of the client that is connecting.

    The NOC uses the passed in GUID as an authentication token for the VES. If the GUID is found in the NOC table of VES clients, the RTS session is authorized for use on behalf of users provisioned by the particular VES installation. If this is the first time a VES has connected, the GUID will not yet be registered. In this case, LicenseID will be used to authenticate the VES as belonging to a particular enterprise license. If the LicenseID is validated, the GUID for the VES will be registered and the RTS session will be authorized for use by any users subsequently provisioned by the VES.

4. The NOC sends down an *ActivateUsers* command to notify the client which users it should be providing with data access.

5. The NOC sends down an *HB* (Hearbeat) command (which also tells the client how soon it should expect the next heartbeat).

6. The NOC sends down a command containing any filter rules set for activated users – this tells the client which new email messages should generate alerts.

7. The NOC sends down a command indicating which, if any, activated users have the ConstantSync feature flag set.

8. The client sends up a *StartupReport* to reflect which users it is capable of providing access for.

4.6 Heartbeats

The NOC periodically sends down heartbeat (HB) commands to test the connection to the client. Each HB contains the time the client should expect the next HB command, so the client can use this to

Exhibit B

determine if the connection to the NOC has broken (if no HB comes by the expected time, the client can assume that the NOC connection is broken and it reconnects to the NOC). To account for network latency, NOC response time, etc, the client has some built-in tolerance for late heartbeats; in general, the client will not disconnect as soon as the heartbeat is expected, but will instead wait for some period of time to see if the heartbeat comes in.

By default, the client assumes the heartbeat interval is 10 seconds, so it should receive the first HB from the NOC within 10 seconds of connecting.

4.7 Data Transfer Operations

RTS data transfers may be triggered by the NOC in the following cases.

1. User interaction with one of the browse interfaces (PC/PDA/WAP) may trigger the NOC to request data from the user's VES for display in a returned HTML/WML page.

2. User submission of a browse interface form may cause the NOC to send some of the POSTed data to the user's VES (sending a new email, saving a contact item, etc.).

3. Batch synchronization (manually invoked or scheduled) by an IMAP/SMTP or SyncML terminal client may trigger two-way transfer of data between VES and the NOC to satisfy the synchronization request.

4. A connected ConstantSync terminal client may send data to the NOC at any time for immediate delivery to the user's VES.

RTS data transfers may be triggered by the VES in the following cases.

1. When a user has configured "new email" alerts to a pager (or other device), the VES will send a new email alert to the NOC for delivery to the alert device. (Supported alert delivery protocols include SMTP, SMS (SMPP), UP-Alerts, and WAP-Push.)

2. When a ConstantSync terminal client is connected to the NOC, VES may send updated data to the NOC for delivery to the client at any time.

The data and command channel connections used to implement these data transfer operations are described in Section 4.3.

Exhibit B

5. Enterprise Network Interaction

The VES component of the VMES solution is designed both for security and for simplicity of installation. To ease installation, VES supports existing enterprise security mechanisms (such as HTTPS proxies) and does not usually require changes to enterprise firewall configurations or deployment of application traffic filtering devices.

5.1 Connectivity Requirements

The network connectivity requirements for VES are similar to those for a typical enterprise workstation. VES must be able to resolve host names, reach the groupware servers it interacts with, and access the Visto NOC.

VES accesses groupware servers through the associated client libraries (MAPI for Exchange access and Lotus Notes C API for Domino access). Therefore the connectivity requirements for VES to reach these servers are generally the same as those of the associated groupware clients (Outlook and Notes).

VES accesses the Visto NOC via one or more SSL connections, which may be made directly over port 443 or may be made through an HTTPS proxy. VES includes support for HTTPS proxies that require username/password authentication.

5.2 Deployment Options

Unlike a typical workstation, to ensure reliable operation, VES should be deployed on a host server located where physical access is restricted to authorized IT personnel (and to ensure that the plug does not get pulled, etc.). In addition, it is recommended that local and remote logon access to the VES server be restricted to personnel with local administrative privileges on the host machine.

There is no requirement that VES be deployed in a DMZ or other specially isolated segment of the enterprise network. However, to facilitate such deployments, when required by enterprise security policies or other considerations, the following section summaries the characteristics of the network connections used by VES.

5.3 Connection Characteristics

VES acts as a client of:

1. The Visto NOC
2. Microsoft Exchange or IBM Lotus Domino
3. A domain name server

VES acts as a server for the Java agents it installs in each provisioned Domino users' mailbox.

VES communicates with these services and agents using IP-based protocols as described in the following sections.

5.3.1 Visto NOC

VES may open up to 21 simultaneous connections to the Visto NOC using SSL on TCP port 443. One of these connections will be kept open long-term and re-made if broken.

Exhibit B

Alternately, if configured to use a proxy, VES may open up to 21 simultaneous connections to an HTTPS proxy on whatever port the proxy uses for HTTP CONNECT connections. Proxies requiring username/password authentication are supported.

5.3.2 Microsoft Exchange Server

The VMES server is a MAPI client (just as the Outlook client is) and in a standard deployment communicates with the Exchange Server using the following services.

- The RCP portmapper service on TCP port 135; and
- Negotiated arbitrary ephemeral ports.

Although not required, it is possible to deploy VES with a firewall between VES and the Exchange server. However, to accommodate the MAPI connection between Exchange and VES in such a deployment, either

- The firewall must be MAPI-aware and thus permit communication on arbitrary ports as negotiated by MAPI; or
- The exchange server must be configured to communicate on static ports and the firewall must be configured to permit access on these ports.

See MSDN: http://support.microsoft.com/kb/155831/EN-US/.

5.3.3 Lotus Domino Server

VES uses both the C API of the notes.dll used by the standard Notes client and the VIM API of the vim.dll. Assuming the default port configuration for Domino is used, the notes.dll connects from VES to Domino on TCP port 1352. VES does not invoke any VIM API methods that create or use network connections.

VES also listens for TCP connections from the Domino server back to the VES. By default, these will be on ports in the range 4000 to 5000. The starting point for this range is configurable.

5.3.4 Domain Name Server

It is assumed that a DNS server is available and accessible from VES.

Exhibit B

6. Browse Access

6.1 Overview

A VMES user may remotely access enterprise data and ISP email from any of the VMES browser-based interfaces. There are three browse access interface variants.

1. The PC browse interface, implemented in HTML.
2. The PDA browse interface, also implemented in HTML, but with no images, frames, Javascript, etc.
3. The WAP browse interface. Implemented in WML.

For a walkthrough of the browse interfaces and details on the features of each, see the *Visto Mobile™ Browser and PC UI Reference Guide.*

Browse-mode access authentication requests are secured via TLS and employ the credentials discussed in the following section. These credentials are protected against dictionary attack by the account lockout feature described in Section 6.3.4.

Confidentiality and integrity of all data transmitted over the Internet is ensured through use of TLS/SSL. See Section 8 for a discussion of the application security measures implemented in the Visto NOC to secure this interface.

6.2 Authentication

The following account credentials are used to authenticate user access to the VMES browse interfaces.

1. Email address: The SMTP address associated with the enterprise email account of the user. This is set by VES at the time the user account is provisioned.

2. MSISDN: A mobile phone number provided by the user during account activation. Once set, this number uniquely identifies the user account and may be used as an alias for the enterprise email address initially used to identify the account.

3. Password: The password string is initially set by VES (randomly generated or set by the VES administrator). The user, via the PC browse interface, may change the password value at any time. Restrictions on allowed password length, character set, etc., vary depending on the particular VMES deployment. The password is used in conjunction with the enterprise email address or MSISDN to authenticate a user for logging in to the VMES browse interface.

3. Secret Question: Browse interface provides a dropdown list of questions for which a user can provide a matching “secret answer.” In cases where the user forgets his or her VMES account password, the secret question/answer can be used to authenticate the user to gain access to the VMES account.

4. Secret Answer: Any alphanumeric string of variable length that the user defines. If successfully used to re-establish access to a VMES account, the user is prompted to choose a new password for the account.

All browse interface authentication requests take the form of an HTTP POST submitted over a connection secured by TLS/SSL (or WTLS in the case of access through a WAP gateway). The Visto NOC server is authenticated to the browser clients by their TLS certificates. The terminal browser is

Exhibit B

authenticated to the server by the submitted email-address/password, MSISDN/password, or secret-question/secret-answer combination. The combinations of email-address/password or MSISDN/password are referred to as the "VMES login credentials."

See Section 8 for a discussion of the security measured used for storage of these credentials at the Visto NOC.

6.3 Logging In and Session Management

6.3.1 Manual Log In

When using a PC or PDA browser to access a VMES account, the user must manually log in to his or her account by entering an account identifier (the user's enterprise email address or MSISDN) and password. Manual login is also required during the first visit to (or after signing out from) VMES via a WAP browser on a mobile phone.

The VMES account login and authentication process is as follows:

1. User enters his or her VMES login credentials (account identifier and password).
2. The Visto NOC looks up the user's profile using the account identifier.
3. A hash is computed by appending the user's salt to the Password entered by the user. The combined data is then run through MD5. (See Section 9 for details on password hashing.)
4. If the new hash and the stored hash match, login to the account is permitted.
5. If the hashes do not match, an error message is displayed and the user must try again.

6.3.2 Persistent Log In

Due to the current limited interfaces on many mobile phones currently on the market, VMES enhances mobile usability by enabling persistent login to user accounts when accessing the account from a phone WAP browser. Using persistent login, a user can quickly re-establish a connection to his or her account and pick up where the user left off during the prior session without having to re-enter his or her login credentials. Security conscious users may sign out of their accounts at the end of each VMES session. Signing out prevents unauthorized access to an account should the user lose his or her mobile device.

To establish a persistent login of a session, the Visto NOC sets an HTTP cookie for the phone. This cookie is stored on the WAP gateway (persistent login requires that the gateway supports cookies). The cookie includes encrypted information including the user's account identifier, the user's account password hash, and information about the specific handset for which the cookie is valid. A "time to live" (TTL) is also factored into the encrypted cookie to restrict the window during which the persistent cookie can be reused.

If the user loses his or her phone and had not signed out of a WAP browser session, the user has two principle options to secure the data:

1. Log in to VMES from another device with Web access and change his or her account password.
2. Contact the VMES administrator to request that the account password be reset.

A new password will block access to the account when a previously set persistent login cookie attempts to establish a new session for the account.

For those gateways that either do not support cookies or do not support cookies in certain circumstances, for example, when a user is roaming across networks, VMES supports persistent login via information in the URLs themselves, so ensuring users maintain connection with a carrier's VMES service.

Exhibit B

Persistent login is not available for the PC or PDA browse access interfaces to VMES. When using a PC or PDA to access VMES, the user must manually log in to the account by entering his or her login credentials. Manual login is also required during the first visit to (or after signing out from) VMES via the WAP browse interface.

6.3.3 Web Session Management

When a user initiates a VMES session from a PC or PDA, the session will stay active until the user manually signs out or until the VMES Server terminates the session because of inactivity. The duration of inactivity before automatic session termination varies depending on the carrier that has deployed VMES, but it is typically set to be 15 minutes. When a session is terminated – manually or due to inactivity – the log in screen is presented; a message displays notifying the user if the session has timed out due to inactivity. To regain access to a session, the user will need to log in again by providing his or her login credentials. The browser's "Back" key cannot be used to regain access to session data. With this protection to access of the user's account in place, no one who has not been authenticated as the user can access a user's prior session when the user has explicitly logged out or if the session has timed out.

6.3.4 Account Lockout

VMES provides the carrier the ability to configure an account lockout to enhance the security against brute force login attempt. The carrier deploying VMES may configure the number of invalid login attempts users are provided before the account is locked. The lockout period is also configurable. Once the account is locked, the user must perform one of the following tasks to gain access to the account:

- Wait the specified lockout period and try again.
- Reset the password by correctly answering the Secret Question.
- Reset the password by contacting their VMES administrator.

Exhibit B

7. Sync Client Access

7.1 Batch Sync Clients

For legacy devices – those that do not support native ConstantSync clients – Visto Mobile 5.2 offers a standards-based approach to providing connectivity.

Devices that support SyncML may use that protocol to synchronize contacts and calendar items. SyncML is deployed as an HTTP-based protocol, protected with industry standard TLS using SSL. This allows both verification of the NOC by the device (by reference to the NOC's certificate) and the creation of a secure link between the two. Authentication of the device by the NOC (by verifying the credentials offered when commencing SyncML) takes place once SSL negotiation is complete and the channel secured. All communication between the NOC and the device is encrypted.

Devices may also use either POP3 or IMAP4 to synchronize email. Where implemented on the device, the communications link may be protected with industry standard TLS using SSL. This allows both verification of the NOC by the device (by reference to the NOC's certificate) and the creation of a secure link between the two. Authentication of the device by the NOC is by verification of the credentials offered when commencing the POP3 or IMAP4 session. All communication between the NOC and device is encrypted if the device requests TLS.

7.2 ConstantSync™ Client

The ConstantSync™ clients are software programs native to a number of popular platforms, including Symbian OS™ (e.g., Nokia Series 60/80 and Sony Ericsson UIQ), Palm, Palm OS®, and Windows Mobile™ Pocket PC and Smartphone. The client detects the presence of a usable wireless network and uses it to maintain a secure, bi-directional push-capable synchronization channel. Synchronized data is held locally on the device so that when the wireless network is not available, access to synchronized data is possible. New data generated while the network is unavailable is queued – both at the device and the VES – and is synchronized when the network is next available. New data generated while the network is available is synchronized immediately.

The device authenticates the identity of the NOC by verifying its SSL certificate. The NOC authenticates the device by checking the user account password it sends. The user account password is protected against brute force and dictionary attacks by a lock-out mechanism that prevents repeated failed tries to guess the password.

The confidentiality “WAP-gap” in the NOC is closed for enterprise data access through use of secure key exchange (ECDH algorithm) and end-to-end data encryption using 128-bit AES. Since ECDH is immune to attack by simply reading the key exchange request and response, the NOC is excluded from being party to the key that results from the key exchange. The use of TLS between the device and the NOC – and between the VES and the NOC – prevents any tampering or “man-in-the-middle” attack from being mounted by any rogue agent on the Internet.

All enterprise application data, whether sent by the device or by the VES, is AES encrypted end-to-end with this key. No enterprise application data – encrypted or otherwise – is ever stored by the NOC, nor is it susceptible to eavesdropping in transit.

7.2.1 ConstantSync™ Terminal Activation

“Device activation” is the means by which a new device is added to the system and subsequently permitted to synchronize the associated user's enterprise data.

Exhibit B

Activation is carried out over an HTTPS-based protocol and is a transaction between the device and the NOC.

The device establishes a TLS/SSL connection with the NOC, verifying the identity of the NOC and establishing a secure communication channel with it. The device issues an HTTP request containing the MSISDN and account password of the user in order that the NOC is able to identify the user and the associated enterprise. The request may also contain optional information (such as the device name and type) in order that user interfaces on the NOC may subsequently refer to this device in a user-friendly manner.

Once the user's identify is verified by the NOC, and permission to activate (or reactivate) the given device is confirmed, the device is granted a unique identifier and is told the address and port upon which the ConstantSync service runs. The device is also informed of the user's Full Name, if known, and the type of service offered under the user's subscription.

The SSL connection is then closed.

7.2.2 ConstantSync™ Connection

Smart devices — such as those based on the Symbian OS™ (including Nokia Series 60/80 and Sony Ericsson UIQ), Palm, Palm OS®, and Windows Mobile™ Pocket PC and Smartphone platforms — can access enterprise data through the NOC via synchronization clients. The Visto sync clients support Push-based synchronization.

When the user's device is turned on, the ConstantSync™ terminal client initiates and maintains an Internet connection with the wireless data network (using PDP Context on GPRS networks or a PPP connection on CDMA 1xRTT networks). Depending on the operator's deployment of VMES, the client may use an operator specific private APN or a public Internet APN.

Transport layer security (TLS) is used to protect all communication between the device and the NOC. The device begins by establishing a TLS/SSL connection with the NOC, and is thus able to verify the identity of the NOC and set up secure communication with it.

The terminal then authenticates itself with the NOC using the user account MSISDN and password and the device identifier established during device activation. The NOC is therefore able to identify the user, the associated enterprise, and the particular device. If authentication is successful, the client maintains an always-on, persistent connection to the NOC.

The device then begins an elliptic curve Diffie-Hellman (ECDH) key exchange with the VES. The ECDH key exchange request is sent via the SSL connection with the NOC, which then forwards the request to the appropriate VES. It is computationally infeasible to deduce the agreed key by monitoring ECDH conversations (hence, even the NOC cannot deduce the end-to-end key agreed between the device and the VES). In addition, the use of SSL in this way prevents rogue agents on the Internet from tampering with the key exchange and mounting a "man-in-the-middle" attack. The VES responds to the key exchange request via the same channel, thus the VES and device are able to agree on a shared secret key. (See Section 11.1.)

Exhibit B

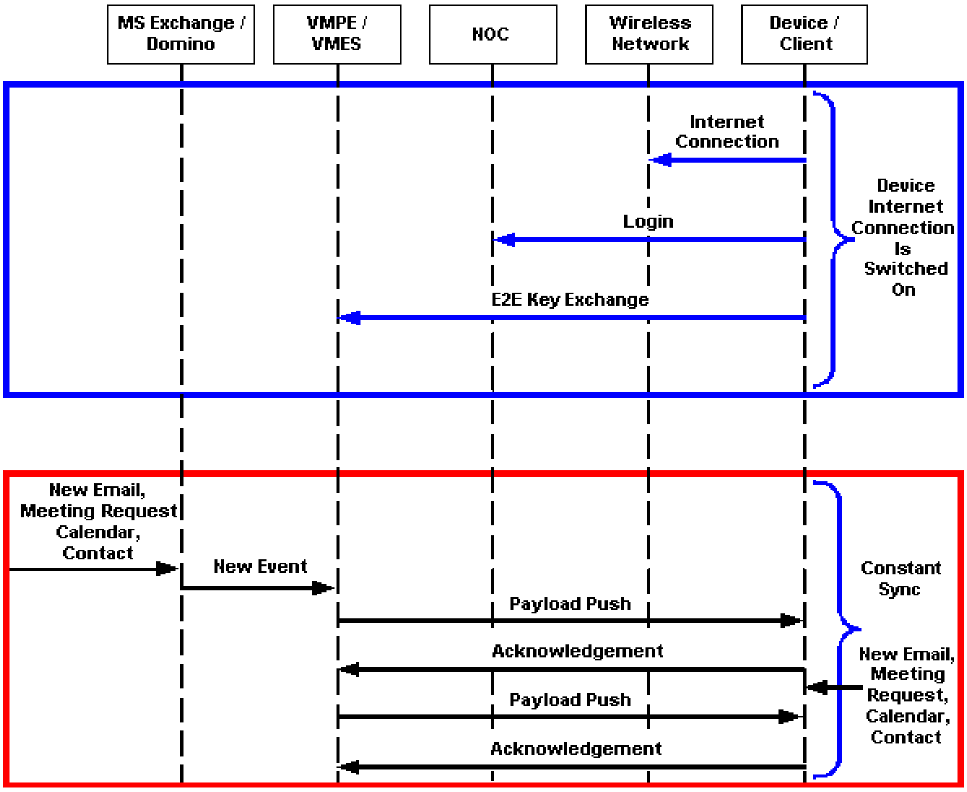

Figure 4: Visto's Implementation of ConstantSync™

7.2.3 ConstantSync™ Data Exchange

Once key exchange is complete, data exchange may begin. When a new event occurs (e.g., new email, meeting request, etc.), the VES detects this new event and communicates directly with the device client by pushing the data payload. Once the device receives the data, an acknowledgement is sent back. Similarly, when a new event occurs (e.g., new email, contact update, etc.) on the device, the device client pushes the data directly to the VES. Once the data is received by the VES, an acknowledgement is sent back to the device client.

Data security is maintained during data exchange between the VES and device (in both directions) through use of 128-bit AES encryption with the agreed upon key. (See Section 11.2.)

7.2.4 J2ME ConstantSync™ Clients

The ConstantSync™ clients implemented for J2ME terminals constitute a special case. These clients do not support the end-to-end AES encryption feature that the ConstantSync™ clients on other platforms use for communication with VES. However, as with other supported clients, all communication between the NOC and the J2ME ConstantSync™ clients is point-to-point encrypted. This provides an equivalent level of security for the J2ME ConstantSync™ clients as is provided for browser-based access and the batch sync clients. This is also equivalent to the security afforded by all ConstantSync™ clients for access through the NOC to ISP based email accounts.

The point-to-point encryption method used by the J2ME ConstantSync™ clients varies depending on the operator deployment and the capabilities of the particular J2ME terminal. When available, TLS/SSL is used to encrypt all traffic between the Visto NOC and the J2ME ConstantSync™ clients.

For J2ME terminals that do not include native support for SSL/TLS, the J2ME clients are configured to use a dedicated APN. Traffic over the wireless link is encrypted using the security features provided by the terminal SIM card. An encrypted VPN tunnel is configured to secure all traffic for the dedicated APN as it is transmitted between the Visto NOC and the wireless operator's network.

Exhibit B

8. The Visto NOC

8.1 Overview

The Visto NOC is based on multiple scalable tiers. These tiers are deployed to provide consistent reliability, high availability, and seamless and flexible scalability in a fully redundant configuration capable of supporting millions of users. Each tier is independent and can scale as needed to support the demands and requirements of that tier.

A load balancer is deployed to ensure scalability and high availability of the Visto NOC by distributing traffic to multiple front-tier application servers. It also maintains real-time awareness of the health of each Application Server. Multiple Application Servers handle incoming HTTP, ConstantSync™ and SyncML traffic from wireless devices, gateways or PCs. They detect the device type and route the browser or the sync connection to the appropriate device template. The Application Servers also run the business logic for transactions being performed. The servers are deployed on an “N+1” basis to support scalability and Availability.

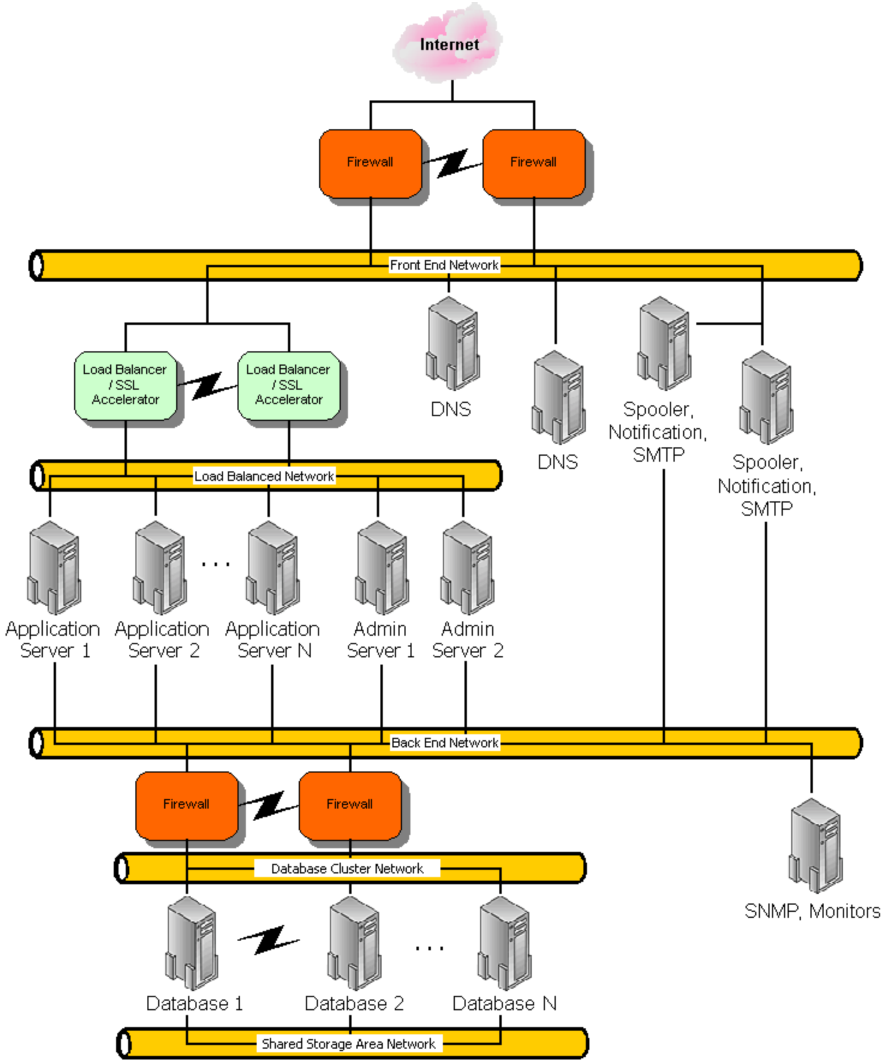

Figure 5: Detailed Scalable System Architecture Diagram

Exhibit B

8.2 Network Configuration

On each front door machine, the Visto NOC uses several ports, which are described below.

Inside Load Balanced IP Ports:

8080:	Unencrypted HTTP data channel /Presentation Layer Server Pool
8081:	Unencrypted HTTP sent from the SSL proxy server running on the Load Balancer Hardware. This is also terminated at the Presentation Layer Server Pool.
8086:	IP Push Server Pool
143:	IMAP Server Pool
25:	SMTP Server Pool
8088:	ConstantSync™ Server Pool
80:	Real-Time Service (enterprise connection) Server Pool

These outside ports are Port Address Translated (PAT) from a load balancer to several Virtual IPs (VIPs). Since the Outside list is open to the world, to protect the Visto NOC Servers the load balancer is fronted by a firewall that only allows standard ports 80/443(http/https), 143/993(IMAP/Secure IMAP), 25/465 (SMTP/Secure SMTP), and 110 (POP – used for ConstantSync) to go through to each VIP. There is no way for intruders to access the Visto database without first compromising one of the Front-tier Application Servers.

Inbound firewall rules prevent malicious scanning on the Application Servers. The network firewall is configured to block and log IP spoofing inbound and outbound. In addition, the firewalls are configured to reject and log ingress traffic from both reserved IP space and IP multicast.

Any outbound queries to ISP servers, provisioning, and other systems go through a Secure Network Address Translation (SNAT) on the load balancer.

Inside (Backnet) IP Inbound:

1200 – 12xx:	RMI (IPC mechanism)
1300 – 13xx:	RMI for Notification

Inside (Backnet) IP Outbound:

1521:	Oracle TNS

The Backnet connections are used for inter-server communication only.

Exhibit B

8.3 Operator Interfaces

The Visto NOC interfaces with several network operator elements such as SMSC, WAP gateway, billing system, authentication system, etc. The following security features are used for these interfaces:

- NOC and operator WAP gateway: HTTPS
- NOC WEB service and browser: HTTPS
- NOC and mobile data network / device clients: 128-bit AES encryption to secure data transmission
- NOC and mobile data network / WAP browser: WTLS
- NOC and operator SMSC: VPN access (i.e., IPSec tunnel)
- NOC and operator backend systems (billing, provisioning, authentication, single sign-on, monitoring, customer care): HTTPS
- IPSec VPN is the only method to administer the NOC hosts remotely

8.4 Availability and Scalability

The Visto NOC deploys Access Control Lists (ACLs) on routers and the network firewall coupled with connection threshold alarms to guard against denial-of-service attacks. To ensure application availability, the Visto NOC uses the Nagios application – a modular-based “polling” system to monitor availability of Visto servers, network devices, and other hardware electronics. Logs from the routers, firewalls, and each application server are collected daily for further routine analysis of potential security problems. Threshold alarms are set on the bandwidth measurement logs to detect problems that arise and automatically notify the Visto NOC site administrators so that they can take corrective actions.

To guard against the possible loss of user data, the NOC has an offsite backup location where sensitive and mission critical data is stored. Backup tapes are stored in a secure safe and offsite vault to protect against theft, destruction, and disclosure of sensitive information.

8.5 Network Access Control

Visto uses industry standard procedures to protect access to the NOC.

- SSH (Secure Shell) is used to interact with each machine.
- The Visto NOC Servers are located in a high security data center with restricted physical access based on multiple levels of authentication for clearance.
- Remote access to the NOC is provided through an IPSec VPN connection and restricted by firewalls/ACLs and password authentication.
- Although multiple operator implementations are collocated on the same network when hosted by Visto, each operator environment is logically isolated from other environments as they consist of separate database table spaces, dedicated application servers, and separate credentials.
- Visto ensures that all network software and systems are current with major security patches for third-party applications. This is done by evaluating each patch based on whether the security exploits apply to application server configuration. If the patch does apply, then it is tested thoroughly and then deployed into production.

Exhibit B

8.6 Administrative Security

Production web support servers have been configured to enforce strict password policies. Unique passwords and IDs are required for access to the network and individual servers. Administrative login credentials are assigned to individuals; administrative login credentials are not shared. They enable logging and auditing of any actions made to the site(s). In addition, when there is no longer a business need for a user account, it is promptly removed from the system. All remote administration is protected with end-to-end encryption using 128-bit SSL.

8.7 Audits and Monitoring

Security and application audit logs are routinely reviewed by the NOC administrators. There are system-level event logs for each major action that serve to answer the question, "who did what, when?" For example:

For root login: SU 08/01 14:32 + pts/13 jthomas-root

Audit logs are retained for seven (7) years. These logs are saved to the storage media and moved to an offsite facility.

8.8 Physical Security

Access to the NOC is limited to those Visto employees with a legitimate business need. When access is permitted, it is logged.. There are several security guards on the premises who monitor the entire NOC via built-in cameras. Every visitor is required to present personal I.D. (e.g., driver's license or passport) and is escorted to Visto equipment by a security representative. Visto's equipment resides in a private cage (virtual Data Center). The cage is secured with a built-in key lock. Individuals granted access to the NOC are required to attend a formal training session at least once a year to be certified on the NOC policies and procedures, as well as receive safety training. Failure to be certified shall result in the loss of access privileges.

8.9 Application Security

The Visto NOC application code includes a number of security measures to thwart attacks against the Web, WAP, ConstantSync™, and other Internet-facing application interfaces. Some of these measures have been discussed in more detail in preceding sections. These measures include the following.

1. The plain text of the user account password and "secret answer" are not stored at the NOC. Instead, hashes of these values are stored. (See Section 9.2.2.)

2. User account credentials are never transmitted unencrypted over the Internet.

3. All user authentication requests are protected against dictionary attack on the user account password by timed lockouts after a configurable number of unsuccessful authentication attempts. (See Section 6.3.4.)

4. Web and WAP session persistence is maintained using a cookie set to a 20 byte random token, which is long enough to be resistant to a dictionary attack. These session persistence tokens are invalidated at the server after sign-off or after a session inactivity timer expires. (See Section 6.3.)

5. Application level checks are done on all requests to verify that the authenticated user owns a given data or resource prior to granting access to that data or resource.

Exhibit B

6. To thwart SQL insertion/injection attacks, the NOC database application user account is not granted direct read or write access to database tables. All application database access must be made through packages of stored procedures.

7. To thwart cross-site scripting attacks, all user-supplied data (whether supplied in request parameters, extracted from the NOC database, or retrieved from an external data server) is escaped before being embedded in HTML / WML pages, including web server error pages.

8. User email, PIM, and file data is not stored or cached at the NOC.

8.10 Roles and Permissions

The following roles are defined within the Visto NOC application.

1. VMES user

   The VMES user is assigned account credentials and may use the user data access interfaces as discussed in previous sections. VMES users may administer some settings of their own account as discussed in the section on User Account Management.

2. VES Administrator

   The VES Administrator is assigned a username and password corresponding to the enterprise license. This credential is used to authorize the VES administrator to download, install, and configure one or more VES installations. VES administrators are not granted access to VMES user application data transmitted through the NOC.

3. Customer Service Representative

   Customer Service Representatives (CSR) manage create and enterprise licenses and may also manage, when necessary, the accounts of individual VMES users. CSRs are assigned a username and password to use in conjunction with the CSR interface and are granted access rights by NOC administrators. Generally, CSR accounts may manage only enterprise licenses created under that same account and VMES users created under those licenses. CSRs administrators are not granted access to VMES user data transmitted through the NOC. VES administrators are not granted access to VMES user application data transmitted through the NOC.

4. NOC Administrator

   NOC Administrators are granted the ability to create and manage all VMES users, enterprise licenses, and CSRs defined for a carrier's VMES deployment. NOC administrators are not granted access to VMES user application data transmitted through the NOC.

5. NOC Operations staff member

   NOC staff members operate the servers that host a carrier's VMES deployment. NOC staff configure and maintain a VMES deployment, but do not have access end-to-end encrypted enterprise data transmitted through the NOC, nor access any stored passwords of VMES users, VES Administrators, CSRs, or NOC administrators.

Exhibit B

9. Data Storage

9.1 VES Local Databases

User profiles and other configuration parameters are stored in the Windows registry.

Table 1: VES Local Databases

Database	Description
User profiles	Stored in Windows registry at [HKEY_LOCAL_MACHINE\SOFTWARE\Visto User Name E-mail address User profile Mailbox profile (for MAPI, X400 address) Mail File (.nsf) for Notes Groupware address
NOC Connection profile	Stored in Windows registry at [HKEY_LOCAL_MACHINE\SOFTWARE\Visto HTTP Proxy credentials Host Username Password (base64 encoded) Port number VES-NOC authentication token VES license id or Enterprise ID NOC connect path
Groupware Connection profile	Stored in Windows registry at [HKEY_LOCAL_MACHINE\SOFTWARE\Visto (MAPI profile name for Exchange Domino admin id file path (.ini) and RC4 encrypted Domino admin key

Exhibit B

9.2 NOC Databases

Table 2: NOC Databases

Database	Description
VES Licenses	Stored in Oracle DB at NOC License id License Admin name, and password (MD5 hashed) Enterprise Level Feature Flags Auth token for each individual VES installation Email address for the license administrator Current user count Maximum allowed number of users per license Suspension code License Expiration date Reseller ID
User profiles	Stored in Oracle DB at NOC License id Contact E-mail address (Contact email address) Enterprise Email address Password (MD5 Hashed) Feature Flags Alert Flags Alert Address First Name Last Name Secret Question Secret Answer (MD5 Hashed) Time zone Code Locale Code Last Login Date/Time Reseller ID Suspension Code Expiration Date Lockout – Failed attempts Lockout – Date of last failed attempt Lockout – Date last Locked Out Audit Columns (date created, date modified, etc.) User Properties (Carrier specific attributes)

Exhibit B

Database	Description
Synchronization state	Stored in Oracle DB at NOC Stored in memory at VES and backed up at NOC. (Permanent MAPI/Notes entry-ids Pending/sync'd/deleted flags Unique Terminal Identifier Terminal mapping of entry-ids Hash of record data (20 Bytes)
ISP email accounts	Stored in Oracle DB at NOC User login name User Password (Encrypted) User Email password Friendly name Mail Signature ISP Login failed attempts Last Login failure date/time Mapping of ISP Mail ID's and associated read status

9.2.1 User Profile Table

As each new VMES account is created, the user's account credentials are added to and securely stored in a table of user profile data in the VMES Servers.

Table 3: User Profile Table

User ID	License ID	Enterprise email address	MSISDN	Salt	Password Hash	Secret Question	Secret Answer Hash
1456	89098989	bob@a.com	2065551212	(8 random bytes)	(16 bytes)	What is your mother's maiden name?	(16 bytes)
8956	19808880	joe@b.com	4255551111	(8 random bytes)	(16 bytes)	What is your pet's name?	(16 bytes)
…			…	…	…	…	…

Exhibit B

9.2.2 Account Password (and User Profile) Management

VMES protects critical user data in the User Profile table using standard hashing algorithms. A salt is used to generate a unique hash for each user. Using a salt prevents intrusion to user accounts using dictionary hash attacks.

Salt: *Eight bytes of random data that are generated for and assigned to each username when an account is created. The salt is applied prior to a hash in order to generate a unique hash for each user.*

VMES uses the industry standard MD5 hashing algorithm to generate a unique representation of the user's password and secret answer. The hash output is 16 bytes (2^{128} bits).

Hash: *The MD5 hashing algorithm is used to convert variable length input into a fixed length (16 byte) output. Output this size makes it virtually impossible for intruders to reverse detect or hack user data.*

MD5(Password + Salt) → 16 bytes of hashed data

Figure 6: Protecting User Profile Information

Benefit: These techniques increase the security of user passwords. Due to the salt and unique hash of the password generated, passwords are never recoverable. Instead, if a user ever forgets his or her password, the user must answer the secret question correctly and then assign a new password to the account. If the user forgets the answer to the secret question or has never set one, they must contact their VES Administrator to reset the password.

9.2.3 ISP Email accounts

To enable users to access their ISP email, VMES stores the password for each mailbox set up on the VMES Servers. The password(s) is stored in the ISP EMail Accounts table along with the server name for the mailbox. To keep the password secure, it is encrypted using the industry standard Blowfish algorithm with a variable-length system key. The key's length is specified and fixed for each carrier deployment to meet security objectives and exportation requirements.

The user can also import from a desktop the Personal Address Book stored in the Windows Address Book, Outlook Express address book, or Outlook. Importing is accomplished using an ActiveX control that is downloaded to the workstation when Internet Explorer is used as the browser. Personal contacts are compressed and thereby obfuscated.

Blowfish: The industry standard encryption algorithm that is used to encrypt all user profile data stored in the VMES Servers. The Internet mailbox passwords are stored and encrypted using the Blowfish algorithm.

System Key: A global encryption key that is used in conjunction with the Blowfish algorithm to encrypt all user profile data in the VMES database, including Internet mailbox credentials. This key is versioned and a new key can be easily rolled out to protect user data if a security breach were ever to occur.

The Internet mailbox password is not hashed so VMES can log in to the user's mail account on his or her behalf.

Exhibit B

10. Summary

10.1 Algorithms

- TLS is used for all Internet connections.
- ECDH is used for key agreement (using curve sect283k1) for ConstantSync™ terminal clients.
- AES is used for data encryption (128-bit key in CFB mode) for exchanges between VES and ConstantSync terminal clients.

10.2 Key Management

- A new AES key is negotiated per ConstantSync™ session.
- AES keys are stored in memory on VES and the terminal client.

10.3 User Account Password Management

- The initial user account password is randomly generated by VES or set by the VES administrator.
- VMES user account passwords are stored in the Visto NOC using a one-way hashing algorithm, which prevents recovery of the original passwords from the NOC database.
- The clear text of user account password may be cached in persistent storage on terminal client.
- The user account password is set and may be reset by VES, but is not stored at VES.
- The user account password may be sent in a welcome e-mail to the user (over internal enterprise e-mail only).
- The user account password may be changed or reset by the user from the PC, PDA or WAP browse interfaces.
- The user may optionally set a secret question and answer to enable the user-initiated password reset feature.
- The user account password is used for terminal authentication.
- Lockouts after unsuccessful authentication attempts protect the user account password and secret answer against online dictionary attacks.

10.4 Security Considerations

- VES registration is authenticated with the enterprise license name and password.
- The VES RTS connection is authenticated to the NOC with a token negotiated during VES registration.
- The NOC is authenticated to VES and the terminals by its TLS certificate.
- All traffic over the Internet secured using TLS (this protects against internet-based attacks such as eavesdropping, man-in-the-middle, offline dictionary, and server impersonation, provides forward secrecy from session to session).
- ECDH key agreement protects the AES key against eavesdropping attacks by someone with access to the NOC.
- AES encryption protects data exchanges between VES and the terminal against eavesdropping attacks by someone with access to the NOC.
- Compromise of an AES key for one ConstantSync™ session does not compromise the data traffic from previous or future sessions (forward secrecy).

Exhibit B

- Enterprise application data is accessed in real-time and not stored outside the firewall.
- The enterprise network login credentials or Exchange/Domino account credentials of individual users are not used by the VMES system.
- Only standard outbound connections are used by VES to enable data access. VMES does not require any “holes’” in enterprise firewalls that can be scanned by malicious intruders.
- All outbound email messages associated with an enterprise email account, but composed from a remote terminal, are routed via the NOC Real-Time Service to the VES for dispatch locally through the enterprise email server.
- The Visto NOC servers are located in a high-security data center with restricted physical access based on multiple levels of authentication and hardware token authentication for clearance.
- In addition to secure firewalls protecting the Visto NOC, the Visto network is under around-the-clock surveillance and monitored for intrusion attempts on a 24x7 basis.

Exhibit B

11. Appendix

11.1 ECDH Key Agreement

After a ConstantSync™ terminal client and VES have negotiated the start of a new ConstantSync session by exchanging WakeUp and WakeUpAck commands, an AES encryption key for the session is negotiated using Elliptic Curve Cryptography Cofactor Diffie-Hellman key agreement (ECDH). This key agreement scheme is classified as C(2,0,ECC CDH) in the NIST *RECOMMENDATION ON KEY ESTABLISHMENT SCHEMES* (Special Publication 800-56).

For key agreement purposes, the ConstantSync™ terminal client and the VES employ the set of 283-bit elliptic curve domain parameters over F_{2^m} associated with a Koblitz curve known as *sect283k1*. This parameter set is defined in *SEC 2: Recommended Elliptic Curve Domain Parameters* and recommended by NIST in FIPS 186-2. As discussed in FIPS 186-2, operations involving this set of domain parameters provide cryptographic strength comparable to that of 128-bit AES.

The key agreement exchange proceeds as follows. All exchanges occur over the secure connection between these endpoints mediated by the Visto NOC.

Table 4: Key Agreement Exchange

Terminal client (T)	Visto NOC	VES (V)
Generate a random value *x*. *x* = RNG()		
Generate an ephemeral private key $d_{e,T}$ and an ephemeral public key $Q_{e,T}$ using the *sect283k1* domain parameters and the random value *x*.		
Send the public key $Q_{e,T}$ to VES.	→ $Q_{e,T}$	
		y = RNG()
		Generate an ephemeral private key $d_{e,V}$ and an ephemeral public key $Q_{e,V}$ using the *sect283k1* domain parameters and the random value *y*.

Exhibit B

Terminal client (T)	Visto NOC	VES (V)
		1. Compute the point $P=h\,d_{e,V}\,Q_{e,T}$. 2. If P=O → Stop 3. $Z=x_P$, where x_P is the x-coordinate of P.
		Calculate the shared 128-bit AES key K to be used for the ConstantSync session. K = KDF(Z)
	$Q_{e,V}$ ←	Send the public key $Q_{e,V}$ to the terminal client.
1. Compute the point $P=h\,d_{e,T}\,Q_{e,V}$. 2. If P=O → Stop 3. $Z=x_P$, where x_P is the x-coordinate of P.		
Calculate the shared 128-bit AES key K K = KDF(Z)		

Here, RNG represents a FIPS 140-2 and ANSI X9.62 compliant random number generator seeded with unpredictable system and/or user input timing data. The scalar *h* is the cofactor parameter (for *sect283k1*, *h*=4). KDF represents the ANSI X9. 63 key derivation function.

11.2 AES encryption and decryption

After session negotiation and key agreement have been completed, all commands and messages exchanged between VES and a ConstantSync terminal client are encrypted using the Advanced Encryption Standard (AES) in the full-block cipher feedback (128-bit CFB) mode, with a randomly generated 128-bit Initializing Vector (*IV*) and the 128-byte session key *K*.

AES is a government-certified, symmetric block-cipher encryption algorithm specified in the Federal Information Processing Standards publication 197 (FIPS-197) issued by the National Institute of Standards and Technology (NIST). It is the latest and most advanced encryption standard, and a replacement for the aging DES standard. AES is a designated encryption algorithm in Federal Information Processing Standard (FIPS), and is compliant with the FIPS 140-1 and 140-2 requirements for cryptographic security.

The functions involved in such an exchange and referenced in the tables below are defined as follows.

1. C_(*X*) is the “deflate” compression of bit string *X*. (See RFC 1951).

2. U_(*X*) is the “deflate” decompression of bit string *X*. (See RFC 1951).

3. E_{*K*}(*IV*, *X*) is the symmetric encryption of data *X* under secret key *K*, using AES in full-block CFB-mode with initialization vector IV.

4. D_{*K*}(IV, *X*) is the symmetric decryption of data *X* under secret key *K*, using AES in full-block CFB-mode with initialization vector IV.

5. A+B is the concatenation of bit strings A and B.

6. H_(*K*, *X*) is the leftmost 10 bytes of the HMAC-SHA1 hash of bit string *X* under key *K*.

The compression and encryption operations involved in transmission of command or message from VES to a ConstantSync™ terminal client are summarized in the table below.

Table 5: Compression and Encryption Operations from VES to Terminal Client

Terminal client (T)	Visto NOC	VES (V)
		Prepare the data block *T* for delivery to the terminal client.
		Compress the data block. *M* = C_(*T*)
		Generate a random 128-bit initialization vector. *IV* = RNG()
		Calculate the message hash. MAC_V = H_(*K*, *M*)
		Encrypt data block M using IV as the initialization vector and K as the key. *X* = E_{*K*}(*IV*,*M*)
	$IV+MAC_V+X$ ←	Send $IV+MAC_V+X$ to the terminal client.
Decrypt the data block *X* using IV as the initialization vector and K as the key. *M* = D_{*K*}(*IV*,*X*)		
Calculate the message hash. MAC_T = H_(*K*, *M*)		
If $MAC_T \neq MAC_V$ → Stop		
Decompress the data block. *T* = U_(*M*)		

Exhibit B

The compression and encryption operations involved in transmission of command or message from a ConstantSync terminal client to VES are summarized as follows.

Table 6: Compression and Encryption Operations from Terminal Client to VES

Terminal client (T)	Visto NOC	VES (V)
Prepare the data block *T* for delivery to VEs.		
Compress the data block. M = C_(T)		
Generate a random 128-bit initialization vector. IV = RNG()		
Calculate the message hash. MAC_T = H_(K, M)		
Encrypt data block M using IV as the initialization vector and *K* as the key. X = E_{K}(IV,M)		
Send IV+MAC_V+X to VES.	→ IV+MAC_T+X	
		Decrypt the data block *X* using *IV* as the initialization vector and *K* as the key. M = D_{K}(IV,X)
		Calculate the message hash. MAC_V = H_(K, M)
		If $MAC_T \neq MAC_V$ → Stop
		Decompress the data block. T = U_(M)

Exhibit B

Visto Documentation Survey

Visto aspires to provide customers with the best quality documentation in our industry. If you have suggestions for improving the quality of this document, please photocopy this page and return it with your comments to the Seattle address on the back cover, **ATTN: Documentation**.

Did you find this document complete?

Is it organized effectively to support your professional tasks?

Are the procedures clearly explained?

Do the illustrations clearly illustrate tasks?

Do you use the document as an online document, as a hardcopy, or both?

Other comments and suggestions:

Exhibit B

VISTO

Corporate Headquarters
Visto Corporation
275 Shoreline Drive
Suite 300
Redwood City, CA, USA 94065
Tel: +1 (650) 486-6000
Fax: +1 (650) 622-9590
www.visto.com

Seattle Office
220 West Mercer
Suite 300
Seattle, WA, USA 98119
Tel: +1 (206) 428-4100
Fax: +1 (206) 428-4101

United Kingdom
Visto Limited
Alexander House
85 Frampton St.
London NW8 8NQ

Data subject to change without notice

Printed in USA, June 2005

Exhibit B